AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

(1.(original) A method for the on-line exchange of content
    data in a secure manner, comprising the steps consisting
    in:
receiving (32) a code entered by a user in an interface device
    (4a-c, 50) linked to a first server device (3) by at
    least one data network (1, 54),
sending (36) a read request from said interface device to said
    first server device in which is stored the respective
    personal cryptographic data of a plurality of users, said
    personal cryptographic data of each user being encrypted
    using a respective authentic code of said user,
receiving (42) the encrypted personal cryptographic data of
    said user in said interface device,
decrypting (44) said personal cryptographic data using said
    entered code when said entered code corresponds to said
    authentic code of the user,
characterized in that it comprises the steps consisting in:
 using (46) said personal cryptographic data to protect an
    exchange of content data (58, 60, 66, 68, 76) between
    said interface device and at least one second server
    device (2a-c) linked to said interface device by at least
    one data network,
erasing (48) said entered code and said personal cryptographic
    data from said interface device.

2.(original) The method as claimed in claim 1, characterized
    in that said interface device and said first server

3

device set up a confidential communication channel
between themselves by sharing at least one encryption key
(Ks) offering a high degree of entropy in relation to
said authentic code of the user, said encrypted personal
cryptographic data ($F_{KP}(D_A)$) being transmitted to said
interface device via said confidential communication
channel.

3. (currently amended) The method as claimed in claim [[1 or]]
2, characterized in that at least one item of personal
code verification data (VP) deriving from said authentic
code of the user (P) according to a deterministic
function (h(N//.)) is stored in said first server device
and in that said first server device explicitly or
implicitly authenticates the interface device using said
personal code verification data item.

4. (original) The method as claimed in claim 3, characterized
in that said deterministic function is a collision-
resistant, irreversible function.

5. (currently amended) The method as claimed in claim 3 ~~2 taken
in combination with claim 3 or~~ 4, characterized in that
said interface device and said first server device
simultaneously handle the sharing of said at least one
encryption key and the explicit or implicit
authentication of said interface device by said first
server device using a Password-Based-Key-Exchange (PBKE)
protocol.

6. (original) The method as claimed in claim 5, characterized
in that said Password-Based-Key-Exchange type protocol
includes a single communication in each direction between
said interface device and said first server device, said

communication from the first server device to the
interface device including the transmission of the
encrypted personal cryptographic data.

7. (currently amended) The method as claimed in ~~one of claims 4~~
~~to 6~~ claim 4, characterized in that said interface device
chooses a first integer (a) corresponding to a first
element (g^a mod p) of a predefined group and said first
server device chooses a second integer (b) corresponding
to a second element (g^b mod p) of said group, then said
interface device and said first server device send each
other said first and second elements, said interface
device and said first server device each producing said
at least one encryption key (Ks) by combining the integer
chosen by itself and the element received by itself, said
first element of the group being transmitted to said
first server device in an encrypted form using a
distinguishing trace (VP) which derives from said code
entered by the user in the interface device according to
said deterministic function, said first element of the
group being decrypted by said first server device using
said personal code verification data (VP), said second
element of the group being transmitted to said interface
device in a form symmetrically encrypted using said
personal code verification data, said second element of
the group being decrypted by said interface device using
said distinguishing trace.

8. (original) The method as claimed in claim 7, characterized
in that said first and second elements of the group are
encrypted with a symmetric encryption protocol (E) which
is chosen such that an attempt to decrypt one of said
elements of the group according to said protocol always

5

produces an element of said group, whatever the data used in said attempt.

9. (currently amended) The method as claimed in ~~one of claims 7 or 8~~ claim 7, characterized in that said first and second elements of the group are encrypted with a symmetric encryption protocol (E) which is chosen such that said integer cannot be obtained from the corresponding encrypted group element.

10. (currently amended) The method as claimed in ~~one of claims 7 to 9~~ claim 7, characterized in that said first element of the group, respectively said second element of the group, is encrypted with a symmetric encryption protocol (E) which comprises the step consisting in composing said element by a composition law of said group with the image of said distinguishing trace, respectively the image of said personal code verification data, by a function with values in said group.

11. (currently amended) The method as claimed in ~~one of claims 1 to 10~~ claim 1, characterized in that said usage step comprises the step consisting in:
authenticating said user with said at least one second server device using the authentication data of said user included in said personal cryptographic data.

12. (currently amended) The method as claimed in ~~one of claims 1 to 11~~ claim 1, characterized in that said usage step comprises the steps consisting in:
receiving content data entered by said user in said interface device,
encrypting said content data using at least one encryption key included in said personal cryptographic data,

sending said encrypted content data (58, 66) to said at least
one second server device (2a-b) to store said encrypted
content data in said second server device and/or transmit
it to a recipient.

13. (currently amended) The method as claimed in ~~one of claims~~
~~1 to 12~~ claim 1, characterized in that said usage step
comprises the steps consisting in:
 sending a second read request specifying content data from
said interface device to said at least one second server
device (2a),
receiving said encrypted content data (60) from said at least
one second server device in said interface device,
decrypting said content data using at least one decryption key
included in said personal cryptographic data.

14. (currently amended) The method as claimed in ~~one of claims~~
~~1 to 13~~ claim 1, characterized in that it comprises the
step consisting in:
 imposing (38) a predefined minimum delay between the
processing of two successive occurrences of said first
read request on the first server device, on pain of not
recognizing the longest delayed occurrence.

15. (currently amended) The method as claimed in ~~one of claims~~
~~1 to 14~~ claim 1, characterized in that it comprises a
step consisting in:
 systematically monitoring (8) communications involving said
first server device (3).

16. (currently amended) The method as claimed in ~~one of claims~~
~~1 to 15~~ claim 1, characterized in that it comprises the
step consisting in:

7

checking the integrity of the personal cryptographic data received from said first server device using integrity control data attached to said personal cryptographic data received from said first server device.

17.(currently amended) The method as claimed in ~~one of claims 1 to 16~~ claim 1, characterized in that it comprises a registration step consisting in:

 providing (11, 12) the personal cryptographic data in said interface device,

receiving (14) an authentic code entered by said user in said interface device,

 encrypting (20) said personal cryptographic data using said authentic code,

sending (24) said encrypted personal cryptographic data from said interface device to said first server device to store said encrypted personal cryptographic data in said first server device,

   erasing (28) said personal cryptographic data and said authentic code from said interface device.

18.(original) The method as claimed in claim 17, characterized in that the registration step comprises the steps consisting in:

   forming (18) personal code verification data from said authentic code,

 sending (24) said personal code verification data from said interface device to said first server device to store said personal code verification data in said first server device.

19.(currently amended) The method as claimed in claim 17 [[or 18]], characterized in that it comprises a step consisting in:

8

rejecting (14) said authentic code entered by the user when said code satisfies predefined evidence criteria.

20. (original) An interface device (4a-c, 50) for the on-line exchange of content data in a secure manner, comprising:
a means for receiving (32) a code entered by a user,
a means for sending (36) a first read request from said interface device to a first server device (3) in which respective personal cryptographic data of a plurality of users is stored, said personal cryptographic data of each user being encrypted using a respective authentic code of said user,
a means for receiving (42) the encrypted personal cryptographic data of said user,
a means for decrypting (44) said personal cryptographic data using said entered code when said entered code corresponds to said authentic code of the user,
characterized by:
means for using (46) said personal cryptographic data to protect an exchange of content data (58, 60, 66, 68, 76) between said interface device and at least one second server device (2a-c),
a means for erasing (48) said code and said personal cryptographic data from said interface device.

21. (original) The device as claimed in claim 20, characterized in that it consists of an electronic mail management program, said means of using the personal cryptographic data comprising a cryptographic module for signing, encrypting and/or decrypting electronic mail using at least some of said personal cryptographic data.

22. (original) The device as claimed in claim 20, characterized in that it consists of a plug-in module suited to an

electronic mail management program comprising a cryptographic module for signing, encrypting and decrypting electronic mail, said means of using the personal cryptographic data comprising a means for providing said cryptographic module with at least some of said personal cryptographic data.

23. (original) A registration interface device (4a-c, 50), characterized in that it comprises:

a means for providing (11, 12) personal cryptographic data in said interface device,

a means (6) for receiving (14) an authentic code entered by said user in said interface device,

a means for encrypting (20) said personal cryptographic data using said authentic code,

a means for sending (24) said encrypted personal cryptographic data from said interface device to a first server device (3) to store said encrypted personal cryptographic data in said first server device, in which the respective personal cryptographic data of a plurality of users is stored, said personal cryptographic data of each user being encrypted using a respective authentic code of said user,

a means for erasing (28) said personal cryptographic data and said authentic code from said interface device.